

Electromagnetic Bombs

Yehoshua Kalisky and Iky Hazan | September 11, 2025

Electromagnetic bombs (EMBs) are weapons based on electromagnetic radiation in the microwave spectrum, with destructive potential against electronic systems including communications, control systems, computers, and electrical systems, up to the point of paralyzing security, economic, and health infrastructures. EMBs have inherent advantages: They operate at the speed of light, are easy to use, cover wide target ranges, and function under all environmental and weather conditions. There are several types of EMBs, and they can be launched from various platforms such as cruise missiles, UAVs, air-dropped munitions, and certain types of rocket and artillery launchers. These bombs pose risks both on land and in space. The State of Israel must urgently prepare to address this emerging threat, particularly by strengthening its defense capabilities for critical national infrastructure. At the same time, it should also consider developing offensive capabilities of this type as a deterrent component that complements existing capabilities.

Background

Electromagnetic bombs (EMBs) are a form of directed energy weapon that employs electromagnetic waves designed to disrupt and destroy electronic systems. The electromagnetic waves generate heat in metallic materials, and their effect is powerful enough to damage and melt metallic conductors in electrical systems. Low-intensity or low-power waves can cause temporary disruptions, while high-intensity waves can destroy systems outright. In most cases, the damage caused by EMBs is electromagnetic rather than kinetic, meaning they leave no physical traces and disable the target without collateral damage. High-power microwaves (HPM) are electromagnetic waves in the frequency range from megahertz or MHz (millions of pulses per second) to gigahertz or GHz (billions of pulses per second). Typically, the operational range for electromagnetic bombs is 1–300 gigahertz, with peak power outputs ranging between 100 megawatts and 100 gigawatts.

Electromagnetic waves penetrate electronic systems through entry points, either external connections like antennas attached to the system or internal connections such as cables, wires, telephone lines, ventilation openings, and faulty shielding that allow access to the inner components of systems. Through these entry points, wave energy can infiltrate and disable a wide range of systems, including telephony, communications, electricity, and security networks, as well as electronic devices like computers, mobile phones, and smartwatches. They can also <u>disable</u> vehicles and military assets such as aircraft, UAVs, drones, tanks, ships, and missile systems. Moreover, microwaves can penetrate and disable underground military

facilities through the communications systems, cables, and antennas connected to them, thus disabling command-and-control centers and even nuclear installations.

The advantages of microwave-based weapons include:

- Operation at the speed of light (300,000 km/second);
- Usability in all weather conditions—even in clouds, rain, fog, or dust;
- Atmospheric effects can be minimized by selecting appropriate wavelengths;
- From an operational standpoint, operating, targeting, and tracking systems are relatively simple due to the wide spatial dispersion of the electromagnetic wave;
- Capability to destroy multiple targets simultaneously, thanks to dispersion and wide coverage;
- Immunity to gravity;
- Ability to either destroy or disrupt targets, depending on the applied frequency and power:
- Minimal collateral damage, as the destructive radius of electromagnetic bombs is usually limited to a few hundred meters around the impact point. Harm to humans is typically limited to just a few meters.

So far, there are no documented cases of operational use of electromagnetic bombs specifically for disabling electronic systems. Nevertheless, related weapons have been used in the past to destroy electronic systems. For example, the United States employed graphite bombs (also known as Blackout Bombs), which disperse graphite fibers to cause short circuits in electrical systems without physically damaging the infrastructure. The first use of graphite bombs occurred during the Gulf War in 1991 when the United States disabled 85% of Iraq's military electricity production. They were later used in the war in Kosovo in 1999, resulting in the collapse of approximately 70% of Serbia's power supply. South Korea is also developing graphite bombs to neutralize electrical systems in North Korea in the event of a future conflict.

Types of Electromagnetic Bombs

There are several methods and technologies for producing and employing electromagnetic bombs. The first method was discovered during early US nuclear experiments in the 1940s. Scientists found that detonating a nuclear bomb at high altitude (at least 30 km) generates an enormous amount of electromagnetic pulses (EMP). These create an electric field capable of disabling electronic systems across hundreds to thousands of kilometers, depending on the altitude of the blast. This article does not address EMPs as a byproduct of nuclear explosions.

Following this discovery, numerous studies examined the mechanisms of EMP effects, eventually leading to the invention of <u>non-nuclear electromagnetic bombs</u>. Unlike nuclear devices, their effective <u>range</u> is far shorter—typically no more than one kilometer. Today, more than <u>20 countries</u>, including the United States, China, and Russia, are developing non-nuclear electromagnetic bombs. Some types are based on relatively simple technical methods that appear in the open academic literature, suggesting that any technologically advanced state could manufacture them.

Non-nuclear electromagnetic bombs are <u>typically divided</u> into two categories: wideband frequency weapons and narrowband frequency weapons. Most current technological development focuses on narrowband applications, which emerged after wideband systems. Narrowband frequency weapons can generally be employed multiple times by firing microwave beams generated from an electrical source over time, targeting specific systems. While they emit a narrower frequency spectrum, they deliver much higher wave intensity and peak power. Narrowband systems produce a concentrated beam at high peak power (hundreds to thousands of kilowatts per pulse), striking targets with precision. They also offer broader operational potential, including the ability to fire hundreds of pulses per second, creating an almost continuous beam capable of striking multiple targets within a short timeframe.

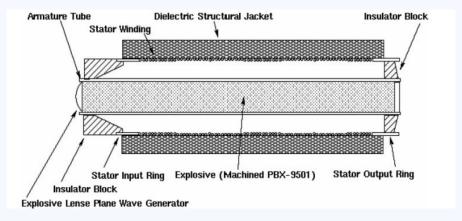
In contrast, wideband frequency weapons are employed against area targets with electronic components vulnerable to a broad range of frequencies. They are expendable munitions—bombs or artillery shells designed for one-time use. Wideband electromagnetic bombs release a large quantity of EMP at once, radiating in all directions and disrupting or neutralizing electronic systems in the blast area. The closer the explosion is to the systems, the stronger the effect—making proximity essential for effective disruption. The waves generated by such explosions carry lower energy (up to tens of joules per pulse) and have limited impact on humans. These bombs can be launched from multiple systems, such as cruise missiles, UAVs, air-dropped munitions, and certain rocket and artillery launchers.

Methods of Producing Non-Nuclear Electromagnetic Bombs

Flux Compression Generator

One method of producing a non-nuclear electromagnetic bomb involves <u>magnetic flux compression</u> (FCG) using an explosive charge (see Figure 1). The device is cylindrical, with an electrical coil and magnet surrounding the cylinder, while the explosive material is located inside. Upon detonation, the explosion causes the magnetic field—usually generated through a current-carrying coil—to collapse and compress. This intensifies the magnetic field, generates a powerful and rapid electrical pulse, and consequently emits multiple electromagnetic pulses in the microwave spectrum across a wide radius of dispersion.

Figure 1. A Schematic Description of a System Based on the Flux Compression Process



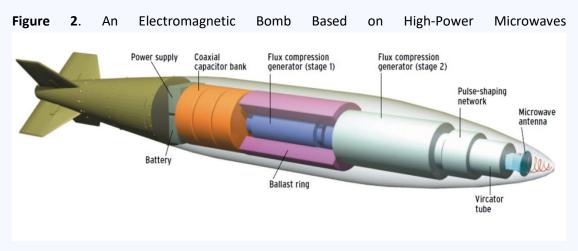
Note. From "High power microwave technology and its military implications," by N. S. Kushwaha and M. M. Sharma, 2008, 2008 International Conference on Recent Advances in Microwave Theory and Applications, https://doi.org/10.1109/AMTA.2008.4763178

Generation of Electromagnetic Waves Using the Magneto-Hydrodynamic Method

Another method for producing wideband electromagnetic bombs employs plasma-driven magneto-hydrodynamic (MHD) generators, powered by explosives or fuel. In MHD generators, a conductor moves through a magnetic field and generates an electric current perpendicular to both the field and the conductor's motion. In this case, the conductor is plasma (atoms with electric charge and electrons) created from ionized explosive material or propellant gas. The electrical charge is collected by electrodes in contact with the plasma jet. Through this process, electromagnetic pulses are produced in the microwave spectrum.

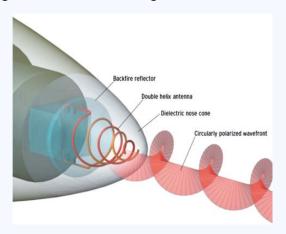
High-Power Microwave Source with Operationally Tuned Frequency

A more advanced method for generating microwaves uses a special device called a <u>vircator</u> (Virtual Cathode Oscillator). This device converts electrical energy into microwaves at extremely high peak power and at a frequency tuned to operational needs. This device works by accelerating a high-current electron beam toward a meshed anode (which collects electrons). Under certain conditions, the electrons passing through the anode form a bubble of electrical charge that oscillates at the chosen microwave frequency. The two most common configurations are the axial vircator, which fires a focused beam and the transverse vircator, which fires a beam dispersed over a wider radius. Figures 2 and 3 illustrate the <u>concept of an electromagnetic bomb based on high-power microwaves</u>.



Note. From "Dawn of the E-Bomb," by M. Abrams, 2003, IEEE Spectrum 40(11), 24–30.

Figure 3. An Electromagnetic Bomb Based on High-Power Microwaves



Note. From "Dawn of the E-Bomb," by M. Abrams, 2003, IEEE Spectrum 40(11), 24–30.

It should be noted that weapons based on high-power microwave sources can also be used for purposes beyond electromagnetic bombs, such as in air defense or crowd control. Moreover, microwave-based systems can be mounted on a wide variety of platforms, including vehicles, ships, aircraft, UAVs, cruise missiles, and ground-based systems.

Optimization of Bomb Efficiency and Maximum Damage

For a bomb to achieve maximum damage, several factors must be considered, including the type of bomb, the output power of the electromagnetic device, the pulse duration of the electromagnetic pulsed energy (commonly referred to as "peak power"), and the adjustment of the range of the electromagnetic radiation frequencies to the types of components being targeted in order to maximize the efficiency of radiation for various purposes or in devices operating across a wide and variable frequency spectrum. Another method of increasing the electromagnetic effect on the target is through precise design of the transmission antenna, taking into account construction materials that can withstand high power levels and dimensions that correspond to the transmitted wavelength.

To strike and damage clusters of targets located within a given area, it is also necessary to optimize the altitude of detonation: The higher the detonation altitude, the greater the area covered by the blast. However, the microwave radiation intensity decreases as altitude increases. Thus, the detonation altitude must be carefully balanced against the desired level of damage.

Table 1 describes the types of damage caused by microwave-based weapons:

Table 1. Types of Damage Caused by Microwave-Based Weapons

Type of Damage	Details	Result
Disruption	, ,	Effect is limited to a specific impact area and only temporary

Degradation	Disruption with minimal damage to electronic systems, sometimes causing system lock-up	Temporary effect; the system does not function for a given period, must be restarted, and occasionally requires minor repairs to return to operation
Damage	Harm to systems and subsystems in order to disable enemy capabilities for a certain period	Can result in permanent or long-term damage, depending on the ability to repair or replace damaged components
Destruction	Severe damage up to complete destruction	Total loss of the enemy's systems, requiring rebuilding of systems and replacement of hardware

Risks from the Use of Electromagnetic Bombs

Risks in the Terrestrial Dimension

There are significant risks associated with the use of electromagnetic bombs (whether conventional or nuclear) if they fall into the wrong hands. Methodologically, it is impossible to fully separate the effects of EMP caused by a nuclear explosion from those of a conventional electromagnetic weapon, although this article focuses only on conventional weapons. The most extreme danger of an electromagnetic bomb was highlighted in a report published in 2014 by the US House of Representatives Homeland Security Committee. The report outlined a worst-case scenario in which the entire electrical grid, electronic systems, and life-sustaining infrastructure in the United States would be disabled for a prolonged period by a nuclear or conventional electromagnetic bomb detonated above the country—leading to mass casualties.

At present, such a scenario is less relevant in Israel's case, both because Israel's adversaries currently lack the ability to acquire a nuclear electromagnetic bomb (although the potential future threat of Iran obtaining nuclear weapons could alter this) and because any nuclear or conventional electromagnetic bomb detonated above Israel would also disable electronic systems across a wide radius beyond Israeli territory. This would affect not only large parts of Israel and its immediate neighbors but also Cyprus, western parts of Saudi Arabia, Iraq, Turkey, and possibly even some Mediterranean European states. All this is in addition to the strategic implications of employing nuclear weapons, even if not detonated directly on the ground.

Another risk raised in the report is the development of small, non-nuclear electromagnetic bombs by non-state actors, enabled by the wide availability of the technology. The report warns that terrorists, criminals, and even individuals could construct small electromagnetic bombs without significant difficulty or cost, using publicly available, unclassified designs from the internet and components purchased in ordinary electronics stores.

In addition to the United States, Russia, China, and North Korea currently possess the ability to carry out nuclear EMP attacks. All three countries have incorporated the use of

electromagnetic bombs into their military doctrines and have developed contingency plans for employing such weapons against the United States. The first nuclear-EMP threat was issued in 1999 during a meeting between a Russian delegation and a US congressional delegation in Vienna, against the backdrop of NATO operations in Yugoslavia. Vladimir Lukin, head of the Russian delegation and former Russian ambassador to the United States, threatened that Russia could launch a nuclear missile from a submarine and detonate it at high altitude, causing widespread destruction of US electronic systems.

Furthermore, <u>a report</u> published in 2020 by the US government's EMP Task Force on National and Homeland Security assessed that China could employ a nuclear or conventional electromagnetic bomb to inflict significant damage on critical US infrastructure, thereby crippling both the American military and economy. The report specifically cited vulnerabilities in communication systems, power stations, military information networks, and even aircraft carriers. As for North Korea, which developed its technology with knowledge shared by Russian experts, the country's state news agency openly <u>declared</u> that the North Korean military has the capability to use a high-altitude hydrogen bomb to disable electronic infrastructure in line with the regime's strategic objectives.

Risks in the Space Dimension

Another potential application of electromagnetic bombs is the attack and interception of satellites. Such weapons could disable a significant portion of commercial and governmental satellite constellations that support daily life on Earth, from cellular communications and online payments to internet browsing. In 2024, <u>US intelligence officials told</u> CNN that Russia is developing a nuclear electromagnetic bomb capable of destroying satellites. According to experts in the field, such a weapon could potentially wipe out vast arrays of small satellites, such as SpaceX's Starlink system, which Ukraine has successfully employed in its war against Russia. It remains unclear whether the system could also damage GPS satellites and nuclear command-and-control satellites, which orbit at higher altitudes. Nonetheless, the use of such a weapon might be a last resort for Russia, since it would also disable Russian satellites located in the same orbital region. China's military is also developing a new system expected to intercept satellites and jam GPS signals, according to a 2024 report in the South China Morning Post. This technology uses optical fibers and synchronizes high-power microwave emissions from seven separate stationary sources into a concentrated narrowband beam with an output of 1 gigawatt.

The Iranian Threat

<u>Iran</u> has also incorporated the use of electromagnetic bombs into its military doctrine. In public military writings, it portrays electromagnetic bombs as a tool of terror and as the ultimate weapon to overcome the West. A <u>report by the US Department of Homeland Security</u> cited an Iranian military journal that declared: "If the world's industrial countries fail to devise effective ways to defend themselves against dangerous electronic assaults, then they will disintegrate within a few years [. . .] American soldiers would not be able to find food to eat, nor would they be able to fire a single shot." Although Iran has not yet succeeded in producing an operational nuclear weapon, it has conducted missile-launch tests simulating a nuclear

electromagnetic bomb attack, including tests of a Shahab-3 missile timed to detonate at high altitude. There are also reports that <u>Iran seeks</u> to develop non-nuclear electromagnetic bombs. Furthermore, according to <u>a report</u> in the Kuwaiti newspaper *Al-Jarida*, Iran has supplied Hezbollah and its other proxies with electromagnetic bombs and missiles carrying electromagnetic warheads.

Widespread use of electromagnetic bombs by Iran or Hezbollah against Israel could disable a substantial portion of Israel's power grid and inflict damage on a wide range of civilian and military facilities, particularly strategic infrastructure. Power disruption could result from strikes on power plants, transmission lines, and generators. Electromagnetic bombs could also damage personal devices such as mobile phones and personal computers, as well as electronic components and communications systems of public services and banking. This would disrupt the functioning of government and emergency agencies, including the police, the ambulance service, and the Fire and Rescue Authority. They could also disable essential electronic systems in hospitals, such as ventilators and medical monitors, thereby endangering human lives. In addition, they could disrupt Israel's water supply by disabling electricity-dependent systems such as desalination plants, water pumping stations, and wastewater treatment facilities. Moreover, electromagnetic pulses could also paralyze transportation platforms cars, trucks, ships, trains, and airplanes—as well as their supporting systems, including air traffic control, railway command-and-control, gas stations, traffic lights, and maritime communication systems. This scenario would also affect supply chains, as any power disruption would cause refrigeration systems to fail, leading to food spoilage.

From a military perspective, electromagnetic bombs could disable systems and platforms that rely on electronic devices, such as fighter jets, server farms, precision munitions, radars, and air-defense systems. In this context, it is worth noting <u>a report</u> in *The Washington Post* stating that Israel eliminated an Iranian-developed electromagnetic bomb.

According to an April 2024 <u>report</u> in the *Daily Star* (not officially confirmed), Israel itself possesses non-nuclear narrowband electromagnetic bombs and reportedly considered using them in a future strike against Iran—although, to the best of our knowledge, this did not occur in the recent war against Iran. The article stated that such an operation could have the potential to devastate strategic infrastructure and military facilities.

The American CHAMP System

Counter-electronics High Power Microwave Advanced Missile Project (CHAMP) is a US project to develop a microwave-based weapon mounted on a cruise missile. The cruise missile enters enemy airspace at low altitude, and the CHAMP system installed on it emits high-power narrowband microwaves that disable electronic systems without causing collateral damage to people or physical infrastructure. The uniqueness of the CHAMP system lies in its ability to fire a focused and precise beam multiple times during a single mission, unlike other electromagnetic bombs that indiscriminately disable all systems in the vicinity with a single strike. The system can also bypass electronic defenses designed to counter classical electromagnetic bombs. The missiles used in the CHAMP system have a range of up to 1,100 km and can be launched from the B-52 strategic bomber. US government officials involved in

the project <u>confirmed</u> that such an operation could also be carried out against North Korea's missile array.

The project was launched in 2009 as part of a collaboration between Boeing's defense arm (Phantom Works) and the Air Force Research Laboratory (AFRL). The electronic components are manufactured by Raytheon, a division of RTX Corporation, while the cruise missiles themselves are produced by Lockheed Martin. In 2012, a successful test of the system was conducted in the Utah desert using an AGM-86 cruise missile launched from a B-52 bomber. During the test, the CHAMP system managed to disable all electronic systems in a two-story building. In 2019, Mary Lou Robinson, head of the High-Power Microwave Division at the Air Force Research Laboratory, confirmed to the Daily Mail that the CHAMP system was operational. (A short video describing the CHAMP system was also released.)

In <u>another article</u> published in the *Daily Mail* in April 2024, US government officials stated that the CHAMP system is capable of destroying or disabling for extended periods facilities connected to Iran's nuclear program—without causing loss of life.

How Does the CHAMP System Work?

- 1. A missile carrying an electromagnetic bomb is launched from a stealth bomber (see Figure 4).
- 2. The missile, equipped with a high-power electromagnetic radiation device in its fuselage, locks onto a predetermined target and generates powerful microwave pulses directed at it.
- 3. Electromagnetic pulses, at a strength of thousands of volts, are aimed at the selected structure, causing lethal voltage surges in electronic devices within seconds.
- 4. These pulses disable power, communications, computers, cell phones, cars, and even tanks. The damage is permanent. Operators of the electromagnetic weapon then conduct monitoring and damage assessment to verify the effectiveness of the bomb.

Missile follows pre-programmed flightpath and is remotely controlled Missile launched from Stealth bomber HOW THE ELECTROMAGNETIC PULSE CANNON WORKS disabling everything inside within a matter of seconds Cannon attached to the undercarriage of missile, which is insulated from Concentrated beam of microwave energy is created by super-powerful microwave oven Pulses of up to thousands of volts aimed at building causing fatal power surge in electronic equipment Wipes out computers. mobile phones, cars and can even disable tanks. Damaged caused is permanent

Figure 4. How the Electromagnetic Pulse Cannon Works

Note. From "Exclusive: U.S. Air Force has deployed 20 missiles..." by R. Kessler, 2019, May 16, Daily Mail, https://www.dailymail.co.uk/news/article-7037549/Air-Force-deployed-20-missiles-fry-military-electronics-North-Korea-Iran.html

HQ controllers observe targets being knocked out

Conclusion and Recommendations

Electromagnetic weapons can disable command-and-control centers, including those located underground, by shutting down communications, computing, surveillance, intelligence, and other electronic systems contained within them—all without causing physical harm to people or infrastructure. Countering such weapons requires substantial investment in effective shielding, particularly to protect critical national infrastructure.

As noted, electromagnetic bombs pose a grave threat to power grids, strategic infrastructure, and electronic devices of all types. Reports of possible acquisition of such weapons by Iran and Hezbollah underscore the urgency of preparing for this threat in the future. Therefore, Israel must act to protect its critical national infrastructure. Various <u>defensive measures</u> already exist to prevent electromagnetic pulses from penetrating electronic devices. The most effective and widely accepted method is Faraday cage shielding, which encloses electronic components or sensitive facilities in a conductive material (typically metal). This blocks electromagnetic fields by dispersing the electrical charge across the surface of the cage and grounding them directly into the earth. Another method is data transmission via fiber

optics, which do not conduct electricity and are immune to EMP effects. Nevertheless, these methods are usually expensive and are not airtight. There is, therefore, a need to develop additional, efficient, and more cost-effective defensive means.

From an offensive standpoint, Israel should independently develop its own electromagnetic weapon systems. At the same time, it should consider purchasing the CHAMP system from the US government at the earliest opportunity—particularly during the Trump administration, which has shown greater flexibility in terms of arms sales to Israel. Such a system could help disable electronic capabilities for a range of purposes, including striking command-and-control centers, shutting down weapons-production facilities and ammunition depots in sensitive areas, and neutralizing launch sites. Should the need arise to prevent the reconstruction of Iran's nuclear facilities, the CHAMP system—or similar systems—could be considered as a complementary means to kinetic strikes.

Editors of the series: Anat Kurz, Eldad Shavit and Ela Greenberg